



AMENDMENTS IN THE SPECIFICATION


Please delete the paragraph beginning at page 3, line 14:

 ~~Figure 5 illustrates a bit-wise view of the mapping section of Fig. 1 in further detail, in accordance with one embodiment.~~

Please amend the paragraph beginning at page 5, line 5 as follows:

 ~~[A-video~~ A video content protection application that uses Km, Kx, An and Mi is described in copending U.S. Patent Applications, serial numbers, ~~<to be inserted>~~ 09/385,590, now issued U.S. Patent No. 6,477,252, and 09/385,592, filed contemporaneously, both entitled "Digital Video Content Transmission Ciphering/Deciphering Method and Apparatus", having common assignee and inventorship with the present application. ~~application.]~~

Please amend the paragraph beginning at page 11, line 5 as follows:

 Referring now back to ~~Fig. 5~~ Fig. 1, recall that a ciphered text may be deciphered by generating the intermediate "keys" and applying them backward. Alternatively, for an embodiment where either the inverse of substitution boxes 604/704 and linear transformation units 606/706 are included or they may be dynamically reconfigured to operate in an inverse manner, the ciphered text may be deciphered as follows. First, the cipher key used to cipher the plain text is loaded into block key section 502, and block key section 502 is advanced by R-1 rounds, i.e. one round short of the number of rounds (R) applied to cipher the plain text. After the initial R-1 rounds, the ciphered text is loaded into data section 504, and both sections, block key section 502 and data section 504, are operated "backward", i.e. with substitution boxes 604/704 and linear transformation units 606/706 applying the inverse substitutions and linear transformations respectively.